(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2002－312316
（P2002－312316A）
(43)公開日　平成14年10月25日(2002.10.25)

(51)Int.Cl.[7]		識別記号	FI		テーマコード（参考）
G06F	15/00	330	G06F	15/00	330A　5B085
	13/00	510		13/00	510S　5J104
G09C	1/00	660	G09C	1/00	660E　5K030
H04L	9/32		H04L	12/22	
	12/22			9/00	671

審査請求　未請求　請求項の数13　ＯＬ　（全 11 頁）

(21)出願番号　特願2001－114891(P2001－114891)

(22)出願日　平成13年４月13日(2001.4.13)

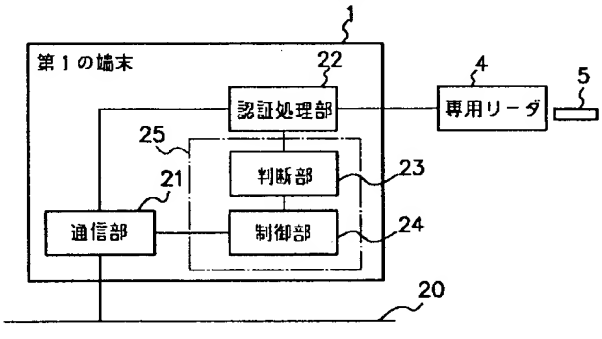
(71)出願人　399104844
住商情報システム株式会社
東京都中央区晴海１丁目８番12号
(72)発明者　加藤　道明
東京都墨田区両国２丁目10番14号　住商情報システム株式会社内
(74)代理人　100105784
弁理士　橘　和之

最終頁に続く

(54)【発明の名称】　不正アクセス防止装置および方法、不正アクセス防止用プログラム、記録媒体

(57)【要約】
【課題】　ユーザ認証が成立した端末を踏み台にして他人が正規利用者になりすますといった不正アクセスを有効に防止できるようにする。
【解決手段】　ネットワーク２０上に接続された第１の端末１に関してユーザ認証が成立しているか否かを判断する判断部２３と、ユーザ認証が成立している間は第１の端末１に対する外部からのアクセスを遮断する（例えば、外部から第１の端末１にアクセス要求が送られてきても応答を返さない）ように制御する制御部２４とを設け、ユーザ認証が成立した第１の端末１が外部から見えないようにして当該端末１をハッキングできないようにし、これにより、ユーザ認証が成立した第１の端末１を踏み台に他人が正規利用者になりすまして目的のシステムに不正にアクセスすることを有効に防止する。

第１の端末の機能構成例



【特許請求の範囲】

【請求項１】　ネットワーク上に接続された端末に関して、上記ネットワークもしくは上記ネットワーク上のシステムにアクセスするのに必要なユーザ認証が成立しているか否かを判断する判断手段と、

上記判断手段により上記ユーザ認証が成立していると判断された場合に、上記端末に対する外部からのアクセスを遮断するように制御する制御手段とを備えたことを特徴とする不正アクセス防止装置。

【請求項２】　ネットワークもしくは上記ネットワーク上のシステムにアクセスするのに必要なユーザ認証を受ける機能を備えた端末に適用する不正アクセス防止装置であって、

上記ネットワークを介して外部から上記端末にアクセス要求が送られてきたときに、上記端末に関して上記ユーザ認証が成立しているか否かを判断する判断手段と、

上記判断手段により上記ユーザ認証が成立していると判断された場合に、上記アクセス要求に対する応答を出力しないように制御する制御手段とを備えたことを特徴とする不正アクセス防止装置。

【請求項３】　上記制御手段は、上記端末に関して上記ユーザ認証が成立している間に、上記ユーザ認証によりアクセスが許可されたシステム以外の外部から上記ネットワークを介して上記端末にアクセス要求が送られてきたときに、上記アクセス要求に対する応答を出力しないように制御することを特徴とする請求項２に記載の不正アクセス防止装置。

【請求項４】　宛先アドレスをもとに経路情報を参照し、転送する次のノードを判断してデータ転送する機能を備えたネットワーク上の中継機器に適用する不正アクセス防止装置であって、

上記ネットワークもしくは上記ネットワーク上のシステムにアクセスするのに必要なユーザ認証を受ける機能を備えた端末に関して、上記ユーザ認証が成立したか否かを判断する判断手段と、

上記判断手段により上記ユーザ認証が成立したと判断されたときに、上記経路情報を退避させ、上記ユーザ認証が成立した端末を宛先とする経路を遮断した第２の経路情報に置き換えるとともに、上記判断手段により上記ユーザ認証が解除されたと判断されたときに、上記第２の経路情報を上記退避しておいた元の経路情報に戻すように制御する制御手段とを備えたことを特徴とする不正アクセス防止装置。

【請求項５】　上記第２の経路情報は、上記ユーザ認証によりアクセスが許可されたシステム以外の外部から上記端末を宛先とした経路を遮断するための経路情報であることを特徴とする請求項４に記載の不正アクセス防止装置。

【請求項６】　ネットワークもしくは上記ネットワーク上のシステムにアクセスするのに必要なユーザ認証を受ける機能を備えた端末に外部から上記ネットワークを介してアクセス要求が送られてきたときに、上記端末に関して上記ユーザ認証が成立しているか否かを判断する第１のステップと、

上記端末に関して上記ユーザ認証が成立していると判断された場合に、上記アクセス要求に対する応答を出力しないように制御する第２のステップとを有することを特徴とする不正アクセス防止方法。

【請求項７】　上記第２のステップでは、上記端末に関して上記ユーザ認証が成立している間に、上記ユーザ認証によりアクセスが許可されたシステム以外の外部から上記ネットワークを介して上記端末にアクセス要求が送られてきたときに、上記アクセス要求に対する応答を出力しないように制御することを特徴とする請求項６に記載の不正アクセス防止方法。

【請求項８】　ネットワークもしくは上記ネットワーク上のシステムにアクセスするのに必要なユーザ認証を受ける機能を備えた端末に関して、上記ユーザ認証の成否を判断する第１のステップと、

上記端末に関して上記ユーザ認証が成立したときに、宛先アドレスをもとに経路情報を参照して次のノードにデータ転送する中継機器の上記経路情報を退避させ、上記ユーザ認証が成立した端末を宛先とする経路を遮断した第２の経路情報に置き換える第２のステップと、

上記端末に関して上記ユーザ認証が解除されたときに、上記第２の経路情報を上記退避しておいた元の経路情報に戻す第３のステップとを有することを特徴とする不正アクセス防止方法。

【請求項９】　上記第２の経路情報は、上記ユーザ認証によりアクセスが許可されたシステム以外の外部から上記端末を宛先とした経路を遮断するための経路情報であることを特徴とする請求項８に記載の不正アクセス防止方法。

【請求項１０】　ネットワーク上に接続された端末に関して、上記ネットワークもしくは上記ネットワーク上のシステムにアクセスするのに必要なユーザ認証が成立しているか否かを判断する判断手段、および上記判断手段により上記ユーザ認証が成立していると判断された場合に、上記端末に対する外部からのアクセスを遮断するように制御する制御手段としてコンピュータを機能させるための不正アクセス防止プログラム。

【請求項１１】　ネットワークもしくは上記ネットワーク上のシステムにアクセスするのに必要なユーザ認証を受ける機能を備えた端末に外部から上記ネットワークを介してアクセス要求が送られてきたときに、上記端末に関して上記ユーザ認証が成立しているか否かを判断する判断手段、および上記判断手段により上記ユーザ認証が成立していると判断された場合に、上記アクセス要求に対する応答を出力しないように制御する制御手段としてコンピュータを機能させるための不正アクセス防止プロ

グラム。
【請求項１２】　ネットワークもしくは上記ネットワーク上のシステムにアクセスするのに必要なユーザ認証を受ける機能を備えた端末に関して、上記ユーザ認証が成立したか否かを判断する判断手段、
上記判断手段により上記ユーザ認証が成立したと判断されたときに、宛先アドレスをもとに経路情報を参照して次のノードにデータ転送する中継機器の上記経路情報を退避させ、上記ユーザ認証が成立した端末を宛先とする経路を遮断した第２の経路情報に置き換える手段、および上記判断手段により上記ユーザ認証が解除されたと判断されたときに、上記第２の経路情報を上記退避しておいた元の経路情報に戻す手段としてコンピュータを機能させるための不正アクセス防止プログラム。
【請求項１３】　請求項１０～１２の何れか１項に記載の各手段としてコンピュータを機能させるためのプログラムを記録したことを特徴とするコンピュータ読み取り可能な記録媒体。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は不正アクセス防止装置および方法、不正アクセス防止用プログラム、記録媒体に関し、例えば、ネットワークもしくは当該ネットワーク上のシステムにアクセスするのに必要なユーザ認証を受ける機能を備えた端末や、宛先アドレスをもとに経路情報を参照し、転送する次のノードを判断してデータ転送する機能を備えたネットワーク上の中継機器に適用して好適なものである。
【０００２】
【従来の技術】近年、インターネットやイントラネットなどのネットワークを利用した情報システムが広く用いられている。この情報システムにおいては、他人による不正侵入、情報漏洩、改ざん、情報システム自体の稼動妨害などをいかに防ぐかが重要な課題となっている。情報システムの安全を守るためのセキュリティシステムとしては幾つかの技術が存在するが、その中の１つに、ユーザ認証技術がある。
【０００３】ユーザ認証技術の代表的なものは、パスワードである。すなわち、個々のユーザが自分に割り当てられた固有のパスワードをキーボードなどから入力し、そのパスワードが個人認証システムにより照合されて正しいことが確かめられると、ネットワークや当該システム上のシステムへのアクセスができるようになるものである。
【０００４】ところが、近年においてはハッキング技術が向上し、パスワードを盗むことは簡単になってきている。そのため、パスワードによるユーザ認証では、他人による不正アクセスを完全に防止することは事実上不可能であった。そこで最近では、解読が困難なＩＣカードを利用したユーザ認証技術も用いられるようになってきている。しかし、このＩＣカードを用いても、そのＩＣカード自体が盗まれてしまうと、他人が正規利用者になりすまして不正にアクセスする恐れがあった。
【０００５】このような実情から、特に最近では、指紋や声、顔などを使って個人を識別する、いわゆるバイオメトリクス認証技術が注目され、開発されている。また、これとＩＣカードとを組み合わせた技術も開発されている。例えば、ユーザの指紋データをＩＣカードに格納しておき、ネットワーク等の利用時にそのＩＣカードを端末に挿入してユーザ本人の指紋データとを照合し、正しければネットワーク等へのアクセスを許可するようにしたものである。
【０００６】
【発明が解決しようとする課題】上述のバイオメトリクス認証技術や、これとＩＣカードとを組み合わせたユーザ認証技術などによれば、従来のパスワードやＩＣカードを単体で用いる場合に比べて、情報システムの安全性を高めることが可能である。しかしながら、ユーザ認証技術をいかに駆使しても、ユーザ認証の成立した端末がハッキングされると、その端末を踏み台にして他人による不正なアクセスが行われてしまうという問題があった。
【０００７】このことを、図８を用いて詳しく説明する。図８に示すシステムでは、第１、第２の端末１０１，１０２と、人事・給与サーバ１０６とがネットワーク１１０を介して接続されている。人事・給与サーバ１０６にはデータベース１０７が接続されており、人事・給与に関する各種データが格納されている。この各種データの中には、個人の学歴・懲罰・病歴・健康状態・給与などに関する個人情報も含まれている。
【０００８】第１、第２の端末１０１，１０２と人事・給与サーバ１０６との間には、個人認証装置１０５が設置されている。個人認証装置１０５は、データベース１０７上のデータが改ざんされたり、個人情報が盗まれたりするといった不都合を回避すべく、人事・給与サーバ１０６に対するアクセスを特定のユーザに対してのみ許可するために、ユーザ認証に関する処理を行うものである。
【０００９】第１の端末１０１には、ＩＣカード１０４の専用リーダ１０３が接続される。ＩＣカード１０４には、人事・給与サーバ１０６に対するアクセス権を有するユーザに関する認証情報（ユーザのステータス情報、あるいは指紋などのバイオ情報等）を格納しておく。
【００１０】第１の端末１０１のユーザがネットワーク１１０を介して人事・給与サーバ１０６にアクセスする場合は、まず、ＩＣカード１０４を専用リーダ１０３に挿入して自分の認証情報を第１の端末１０１に読み取らせる。第１の端末１０１は、読み取った認証情報を個人認証装置１０５に送る。個人認証装置１０５は、第１の端末１０１から送られてきた認証情報を確認し、正しけ

れば人事・給与サーバ１０６へのアクセスを許可する。

【００１１】このようにして第１の端末１０１にユーザ認証が成立すると、当該第１の端末１０１から個人認証装置１０５を介して人事・給与サーバ１０６に至るパスが形成される。この状態で、第２の端末１０２から第１の端末１０１がハッキングされると、第１の端末１０１を踏み台にして第２の端末１０２のユーザが第１の端末１のユーザになりすまし、人事・給与サーバ１０６に不正にアクセスすることが可能となってしまう。

【００１２】このように、従来は、ユーザ認証技術自体は改良が加えられ、正規利用者以外の他人がユーザ認証を受けることは困難になってきている。しかし、正規利用者によってユーザ認証の成立した端末をハッキングすることにより、当該端末を踏み台にして他人が正規利用者になりすますことが可能となってしまう。そのため、ネットワークや当該ネットワーク上のシステムに対する他人による不正アクセスを完全に防ぐことはできなかった。

【００１３】本発明は、このような問題を解決するために成されたものであり、ユーザ認証が成立した端末を踏み台にして他人が正規利用者になりすますといった不正アクセスを有効に防止できるようにすることを目的とする。

【００１４】

【課題を解決するための手段】本発明の不正アクセス防止装置は、ネットワーク上に接続された端末に関して、上記ネットワークもしくは上記ネットワーク上のシステムにアクセスするのに必要なユーザ認証が成立しているか否かを判断する判断手段と、上記判断手段により上記ユーザ認証が成立していると判断された場合に、上記端末に対する外部からのアクセスを遮断するように制御する制御手段とを備えたことを特徴とする。

【００１５】本発明の他の態様では、ネットワークもしくは上記ネットワーク上のシステムにアクセスするのに必要なユーザ認証を受ける機能を備えた端末に適用する不正アクセス防止装置であって、上記ネットワークを介して外部から上記端末にアクセス要求が送られてきたときに、上記端末に関して上記ユーザ認証が成立しているか否かを判断する判断手段と、上記判断手段により上記ユーザ認証が成立していると判断された場合に、上記アクセス要求に対する応答を出力しないように制御する制御手段とを備えたことを特徴とする。

【００１６】本発明のその他の態様では、上記制御手段は、上記端末に関して上記ユーザ認証が成立している間に、上記ユーザ認証によりアクセスが許可されたシステム以外の外部から上記ネットワークを介して上記端末にアクセス要求が送られてきたときに、上記アクセス要求に対する応答を出力しないように制御することを特徴とする。

【００１７】本発明のその他の態様では、宛先アドレスをもとに経路情報を参照し、転送する次のノードを判断してデータ転送する機能を備えたネットワーク上の中継機器に適用する不正アクセス防止装置であって、上記ネットワークもしくは上記ネットワーク上のシステムにアクセスするのに必要なユーザ認証を受ける機能を備えた端末に関して、上記ユーザ認証が成立したか否かを判断する判断手段と、上記判断手段により上記ユーザ認証が成立したと判断されたときに、上記経路情報を退避させ、上記ユーザ認証が成立した端末を宛先とする経路を遮断した第２の経路情報に置き換えるとともに、上記判断手段により上記ユーザ認証が解除されたと判断されたときに、上記第２の経路情報を上記退避しておいた元の経路情報に戻すように制御する制御手段とを備えたことを特徴とする。

【００１８】本発明のその他の態様では、上記第２の経路情報は、上記ユーザ認証によりアクセスが許可されたシステム以外の外部から上記端末を宛先とした経路を遮断するための経路情報であることを特徴とする。

【００１９】また、本発明の不正アクセス防止方法は、ネットワークもしくは上記ネットワーク上のシステムにアクセスするのに必要なユーザ認証を受ける機能を備えた端末に外部から上記ネットワークを介してアクセス要求が送られてきたときに、上記端末に関して上記ユーザ認証が成立しているか否かを判断する第１のステップと、上記端末に関して上記ユーザ認証が成立していると判断された場合に、上記アクセス要求に対する応答を出力しないように制御する第２のステップとを有することを特徴とする。

【００２０】本発明の他の態様では、上記第２のステップでは、上記端末に関して上記ユーザ認証が成立している間に、上記ユーザ認証によりアクセスが許可されたシステム以外の外部から上記ネットワークを介して上記端末にアクセス要求が送られてきたときに、上記アクセス要求に対する応答を出力しないように制御することを特徴とする。

【００２１】本発明のその他の態様では、ネットワークもしくは上記ネットワーク上のシステムにアクセスするのに必要なユーザ認証を受ける機能を備えた端末に関して、上記ユーザ認証の成否を判断する第１のステップと、上記端末に関して上記ユーザ認証が成立したときに、宛先アドレスをもとに経路情報を参照して次のノードにデータ転送する中継機器の上記経路情報を退避させ、上記ユーザ認証が成立した端末を宛先とする経路を遮断した第２の経路情報に置き換える第２のステップと、上記端末に関して上記ユーザ認証が解除されたときに、上記第２の経路情報を上記退避しておいた元の経路情報に戻す第３のステップとを有することを特徴とする。

【００２２】本発明のその他の態様では、上記第２の経路情報は、上記ユーザ認証によりアクセスが許可された

システム以外の外部から上記端末を宛先とした経路を遮断するための経路情報であることを特徴とする。

【００２３】また、本発明の不正アクセス防止プログラムは、ネットワーク上に接続された端末に関して、上記ネットワークもしくは上記ネットワーク上のシステムにアクセスするのに必要なユーザ認証が成立しているか否かを判断する判断手段、および上記判断手段により上記ユーザ認証が成立していると判断された場合に、上記端末に対する外部からのアクセスを遮断するように制御する制御手段としてコンピュータを機能させるためのものである。

【００２４】本発明の他の態様では、ネットワークもしくは上記ネットワーク上のシステムにアクセスするのに必要なユーザ認証を受ける機能を備えた端末に外部から上記ネットワークを介してアクセス要求が送られてきたときに、上記端末に関して上記ユーザ認証が成立しているか否かを判断する判断手段、および上記判断手段により上記ユーザ認証が成立していると判断された場合に、上記アクセス要求に対する応答を出力しないように制御する制御手段としてコンピュータを機能させることを特徴とする。

【００２５】本発明のその他の態様では、ネットワークもしくは上記ネットワーク上のシステムにアクセスするのに必要なユーザ認証を受ける機能を備えた端末に関して、上記ユーザ認証が成立したか否かを判断する判断手段、上記判断手段により上記ユーザ認証が成立したと判断されたときに、宛先アドレスをもとに経路情報を参照して次のノードにデータ転送する中継機器の上記経路情報を退避させ、上記ユーザ認証が成立した端末を宛先とする経路を遮断した第２の経路情報に置き換える手段、および上記判断手段により上記ユーザ認証が解除されたと判断されたときに、上記第２の経路情報を上記退避しておいた元の経路情報に戻す手段としてコンピュータを機能させることを特徴とする。

【００２６】また、本発明のコンピュータ読み取り可能な記録媒体は、請求項１０～１２の何れか１項に記載の各手段としてコンピュータを機能させるためのプログラムを記録したことを特徴とする。

【００２７】

【発明の実施の形態】（第１の実施形態）以下、本発明の第１の実施形態を図面に基づいて説明する。図１は、本実施形態による不正アクセス防止装置を適用したネットワークシステム全体の構成を示す図である。

【００２８】図１において、１，２，３はパーソナルコンピュータ等から成る端末、９はファイルサーバ、１０はメールサーバ、１１は人事・給与サーバ、１２は経理・財務サーバであり、これらがネットワーク２０を介して互いに通信可能なように接続されている。

【００２９】ファイルサーバ９は、ファイルの転送、削除、ディレクトリ操作などの処理を行う。メールサーバ１０は、端末１，２，３からの要求に基づいて電子メールを送信したり、届いた電子メールを保管して端末１，２，３からの照会があったときに引き渡したりする処理を行う。人事・給与サーバ１１は、企業内の人事・給与に関する様々な処理を行う。経理・財務サーバ１２は、企業内の経理・財務に関する様々な処理を行う。なお、これらの各種サーバ９～１２は公知のものを用いることが可能であるので、ここでは処理内容の詳細な説明は割愛する。

【００３０】８はルータであり、ネットワーク２０上の適当な位置に設置されている。あるコンピュータからネットワーク２０上に送信されたデータは、必ずルータ８を経由して目的とするコンピュータに届けられる。このルータ８は、ＩＰヘッダにある宛先ＩＰアドレスをもとに、ルータ８自身が持つ経路情報（ルーティングテーブル）を参照し、転送する次のノードを判断してデータを転送する。

【００３１】１３は個人認証装置であり、第１～第３の端末１～３と、人事・給与サーバ１１および経理・財務サーバ１２との間に設置されている。個人認証装置１３は、人事・給与サーバ１１、経理・財務サーバ１２に対するアクセスを特定のユーザに対してのみ許可するために、第１および第２の端末１，２から送られてくる認証情報に基づいてユーザ認証に関する処理を行う。

【００３２】第１の端末１には、ＩＣカード５の専用リーダ４が接続される。ＩＣカード５には、例えば人事・給与サーバ１１に対するアクセス権を有するユーザに関する認証情報（ユーザのステータス情報、あるいは指紋などのバイオ情報等）を格納しておく。第１の端末１のユーザは、ファイルサーバ９とメールサーバ１０とに自由にアクセスすることができるとともに、ＩＣカード５を用いてユーザ認証を受けることで、人事・給与サーバ１１にもアクセスできるようになる。

【００３３】第１の端末１のユーザが人事・給与サーバ１１にアクセスする場合は、まず、ＩＣカード５を専用リーダ４に挿入して自分の認証情報を第１の端末１に読み取らせる。第１の端末１は、読み取った認証情報をルータ８を介して個人認証装置１３に送る。個人認証装置１３は、第１の端末１から送られてきた認証情報を確認し、正しければ人事・給与サーバ１１へのアクセスを許可する。

【００３４】また、第２の端末２には、ＩＣカード７の専用リーダ６が接続される。ＩＣカード７には、例えば経理・財務サーバ１２に対するアクセス権を有するユーザに関する認証情報（ユーザのステータス情報、あるいは指紋などのバイオ情報等）を格納しておく。第２の端末２のユーザは、ファイルサーバ９とメールサーバ１０とに自由にアクセスすることができるとともに、ＩＣカード７を用いてユーザ認証を受けることで、経理・財務サーバ１２にもアクセスできるようになる。

【００３５】第２の端末２のユーザが経理・財務サーバ１２にアクセスする場合は、まず、ＩＣカード７を専用リーダ６に挿入して自分の認証情報を第２の端末２に読み取らせる。第２の端末２は、読み取った認証情報をルータ８を介して個人認証装置１３に送る。個人認証装置１３は、第２の端末２から送られてきた認証情報を確認し、正しければ経理・財務サーバ１２へのアクセスを許可する。

【００３６】第３の端末３は、ユーザ認証を受けるための機能を備えていない。すなわち、第３の端末３のユーザは、人事・給与サーバ１１および経理・財務サーバ１２に対するアクセス権を持っておらず、ファイルサーバ９とメールサーバ１０に対してのみアクセスすることが可能である。

【００３７】なお、ここでは第１および第２の端末１，２の外付けでＩＣカード５，７の専用リーダ４，６を設ける構成としたが、第１および第２の端末１，２自体がＩＣカード５，７の読み取り機能を備えていても良い。また、ここではユーザ認証を受けるためにＩＣカード５，７を用いているが、本発明はユーザ認証の方法は特に限定しない。例えば、パスワードなどの他のユーザ認証技術を用いても良い。

【００３８】また、ここでは、アクセスするのにユーザ認証を必要とするものを人事・給与サーバ１１および経理・財務サーバ１２としたが、これらのサーバに限定されるものではない。例えば、図示しない他のサーバもしくはファイルサーバ９やメールサーバ１０、または図示しないホストコンピュータなどについても、個人認証装置１３によるユーザ認証をアクセスの前提条件とするようにしても良い。

【００３９】図２は、第１の端末１の機能構成例を示すブロック図である。なお、第２の端末２も第１の端末１と同様に構成されるので、ここでは図示を省略する。図２において、２１は通信部であり、ネットワーク２０を介してデータの送受信に関する処理を行う。２２は認証処理部であり、個人認証装置１３と共動してユーザ認証に関する処理を行う。

【００４０】上記認証処理部２２は、専用リーダ４にて読み取ったＩＣカード５内の認証情報を取り込み、通信部２１を介して個人認証装置１３に送信する機能を有している。また、個人認証装置１３から通信部２１を介して送られてくる認証許可情報を取り込み、保持する機能も有している。認証処理部２２が認証許可情報を保持している間だけ、人事・給与サーバ１１にアクセスすることが可能である。

【００４１】２３は判断部であり、外部からネットワーク２０を介して通信部２１にアクセス要求が送られてきたときに、認証処理部２２により認証許可情報が保持されているかどうかを見ることによって、第１の端末１に関してユーザ認証が成立しているか否かを判断する。

【００４２】なお、ここでは認証処理部２２に認証許可情報を保持させ、当該情報の有無によってユーザ認証の成否を判断しているが、本発明はこの例に限定されるものではない。例えば、外部からアクセス要求が送られてきたときに、通信部２１を介して個人認証装置１３にユーザ認証の成否を問い合わせるようにしても良い。この場合は、個人認証装置１３が認証許可情報を保持することになる。

【００４３】２４は制御部であり、第１の端末１に関してユーザ認証が成立している間に、外部からネットワーク２０を介して第１の端末１にアクセス要求が送られてきたときは、そのアクセス要求に対する応答を通信部２１から出力しないように制御する。一方、第１の端末１に関してユーザ認証が成立していないときは、通常通り、外部からのアクセス要求に対して応答を出力するように制御する。

【００４４】上記判断部２３および制御部２４によって、本実施形態の不正アクセス防止装置２５が構成される。この不正アクセス防止装置２５は、実際には第１の端末１のＣＰＵあるいはＭＰＵ、ＲＡＭ、ＲＯＭなどで構成され、ＲＡＭやＲＯＭに記憶されたプログラムが動作することによって上述した判断部２３および制御部２４の機能構成が実現される。

【００４５】したがって、第１の端末１が上記判断部２３および制御部２４の機能を果たすように動作させるプログラムを例えばＣＤ－ＲＯＭのような記録媒体に記録し、コンピュータに読み込ませることによって実現できるものである。上記プログラムを記録する記録媒体としては、ＣＤ－ＲＯＭ以外に、フロッピー（登録商標）ディスク、ハードディスク、磁気テープ、光ディスク、光磁気ディスク、ＤＶＤ、不揮発性メモリカード等を用いることができる。また、上記プログラムをネットワーク２０を介して他のコンピュータからダウンロードするようにしても良い。

【００４６】また、第１の端末１が供給されたプログラムを実行することにより判断部２３および制御部２４の機能が実現されるだけでなく、そのプログラムが第１の端末１において稼働しているＯＳ（オペレーティングシステム）あるいは他のアプリケーションソフト等と共同して上述の機能が実現される場合や、供給されたプログラムの処理の全てあるいは一部が第１の端末１の機能拡張ボードや機能拡張ユニットにより行われて上述の機能が実現される場合も、かかるプログラムは本発明の実施形態に含まれる。

【００４７】図３は、一般的な通信プロトコルを示す図である。送信側から受信側にデータを送信する場合は、まず、送信側から受信側にデータ送信を開始することを伝える信号ＳＴＡＲＴを送る。これに対応して受信側から送信側に応答信号Ａｃｋが返されると、送信側から受信側にデータＤａｔａが送られる。データ送信が終了す

ると、送信側から受信側にデータ送信が終了したことを伝える信号ＥＮＤを送る。これに対応して受信側から送信側に応答信号Ａｃｋを返すことにより、一連のデータ通信が完了する。

【００４８】このような通信プロトコルにおいて、制御部２４は、第１の端末１に関してユーザ認証が成立している間に、アクセス要求であるデータ送信開始信号ＳＴＡＲＴが外部から送られてきたときは、それに対する応答信号Ａｃｋを返さないように制御する。このようにすることで、アクセス要求元に対して、第１の端末１はあたかもネットワーク２０上に存在していないように見せることが可能となる。

【００４９】通常、ユーザ認証が成立している第１の端末１に対するハッキングは、外部から第１の端末１に仮のデータを送るなどして、第１の端末１のネットワーク２０上における存在位置を確認することによって行われる。しかし、本実施形態によれば、第１の端末１は、ユーザ認証が成立している間は外部からのアクセス要求に対して応答を返さないので、外部から第１の端末１の存在を知ることはできず、第１の端末１にアクセスすることは一切できなくなる。

【００５０】したがって、例えば第３の端末３からユーザ認証が成立した第１の端末１をハッキングすることは全くできなくなり、第１の端末１を踏み台にして他人が第１の端末１のユーザになりすますことによる人事・給与サーバ１１への不正アクセスを有効に防止することができる。同様に、ユーザ認証が成立した第２の端末２をハッキングすることもできなくなり、第２の端末２を踏み台にした経理・財務サーバ１２への不正アクセスも有効に防止することができる。

【００５１】以上の例では、例えば第１の端末１に関してユーザ認証が成立している間は、第１の端末１から人事・給与サーバ１１にアクセスすることは可能であるが、逆に人事・給与サーバ１１から第１の端末１にアクセスすることはできなくなる。しかし、例えば夜間にタイマをセットして、人事・給与サーバ１１から起動して第１の端末１に所望のデータを送って印刷をするといった要求も存在する。

【００５２】このような要求に対応するために、第１の端末１に関してユーザ認証が成立している間でも、ユーザ認証によりアクセスが許可された人事・給与サーバ１１からのアクセスだけは許可する（応答信号Ａｃｋを返す）ようにすることも可能である。すなわち、この場合の制御部２４は、人事・給与サーバ１１以外のコンピュータからネットワーク２０を介して第１の端末１にアクセス要求が送られてきたときに、そのアクセス要求に対する応答を出力しないように制御する。

【００５３】図４は、この場合の第１の端末１に備えられる不正アクセス防止装置２５の動作を示すフローチャートである。図４において、制御部２４は、通信部２１が外部からデータ送信開始信号ＳＴＡＲＴを受信したかどうかを監視し（ステップＳ１）、これを受信した場合には、判断部２３を用いて、現在第１の端末１に関してユーザ認証が成立しているかどうかを判定する（ステップＳ２）。

【００５４】現在ユーザ認証が成立していない場合は、たとえ第１の端末１がハッキングされても、当該第１の端末１を踏み台にして人事・給与サーバ１１にアクセスすることは不可能であるから、通常通り応答信号Ａｃｋを返すように通信部２１を制御する（ステップＳ５）。これにより、第１の端末１に対して外部から自由にアクセスすることが可能となる。

【００５５】一方、現在ユーザ認証が成立している場合には、制御部２４は、アクセス要求元（データ送信開始信号ＳＴＡＲＴの発信元）が人事・給与サーバ１１であるかどうかを判定する（ステップＳ３）。本実施形態のようにＩＣカード５を使ってユーザ認証を行う場合、そのＩＣカード５に認証情報を設定する上で、人事・給与サーバ１１のＩＰアドレスも保持される。したがって、ＩＣカード５から読み取ったＩＰアドレスと、データ送信開始信号ＳＴＡＲＴと共に送られてくるＩＰアドレスとが一致するかどうかを見ることによって、アクセス要求元が人事・給与サーバ１１であるかどうかを判定することが可能である。

【００５６】アクセス要求元が人事・給与サーバ１１でなかった場合は、制御部２４は、データ送信開始信号ＳＴＡＲＴに対して応答信号Ａｃｋを返さないように通信部２１を制御する（ステップＳ４）。これにより、第１の端末１が外部から見えないようにし、第１の端末１を踏み台にした人事・給与サーバ１１への不正アクセスを防止する。

【００５７】また、アクセス要求元が人事・給与サーバ１１であった場合は、制御部２４は、データ送信開始信号ＳＴＡＲＴに対して応答信号Ａｃｋを返すように通信部２１を制御する（ステップＳ５）。これにより、第１の端末１に対して人事・給与サーバ１１から自由にアクセスすることが可能となる。

【００５８】以上詳しく説明したように、第１の実施形態においては、第１および第２の端末１，２に関してユーザ認証が成立している間は、これらの端末１，２に対する外部からのアクセスを遮断するように制御しているので、第１および第２の端末１，２をハッキングすることができないようにすることができる。これにより、第１および第２の端末１，２を踏み台にして他人が個人認証装置１３を通過し、人事・給与サーバ１１や経理・財務サーバ１２などに不正にアクセスすることを有効に防止することができる。

【００５９】（第２の実施形態）次に、本発明の第２の実施形態を図面に基づいて説明する。第２の実施形態による不正アクセス防止装置を適用したネットワークシス

テム全体の構成は、図１と同様である。ただし、第１および第２の端末１，２は、図２に示した不正アクセス防止装置２５の機能構成を備えていない。本実施形態において不正アクセス防止装置は、ルータ８内に設けられる。

【００６０】図５は、ルータ８の機能構成例を示すブロック図である。図５において、３１は通信部であり、ネットワーク２０を介してデータ転送に関する処理を行う。すなわち、ネットワーク２０を介して送られてきたデータのＩＰヘッダにある宛先ＩＰアドレスをもとに、経路情報メモリ３５に保持されている経路情報（ルーティングテーブル）を参照し、転送する次のノードを判断してデータを転送する。

【００６１】３２は判断部であり、第１の端末１および第２の端末２に関するユーザ認証の成否を判断する。第１および第２の端末１，２でユーザ認証を受ける場合は、これらの端末１，２と個人認証装置１３との間で、ルータ８を経由してユーザ認証に必要なデータがやり取りされる。したがって、ユーザ認証の実行の際にルータ８の通信部３１を介してやり取りされるデータを判断部３２が監視することによって、ユーザ認証が成立したことや、その後ユーザ認証が解除されたことを確認することが可能である。

【００６２】なお、第１および第２の端末１，２に関するユーザ認証の成否を判断する手法は、これに限定されない。例えば、第１および第２の端末１，２でユーザ認証が成立もしくは解除されたときに、そのことを第１および第２の端末１，２からルータ８に明示的に伝えるようにしても良い。

【００６３】３３は制御部であり、判断部３２により第１の端末１あるいは第２の端末２に関してユーザ認証が成立したと判断されたときに、経路情報メモリ３５内の経路情報を退避メモリ３６に退避させ、ユーザ認証が成立した端末を宛先とする経路を遮断した第２の経路情報に、経路情報メモリ３５の内容を置き換える。また、ユーザ認証が解除されたと判断されたときに、退避メモリ３６に退避しておいた元の経路情報を経路情報メモリ３５に戻すように制御する。

【００６４】上記判断部３２および制御部３３によって、本実施形態の不正アクセス防止装置３４が構成される。この不正アクセス防止装置３４は、実際にはルータ８のＣＰＵあるいはＭＰＵ、ＲＡＭ、ＲＯＭなどで構成され、ＲＡＭやＲＯＭに記憶されたプログラムが動作することによって上述した判断部３２および制御部３３の機能構成が実現される。

【００６５】図６は、経路情報の置き換え例を示す図である。図６（ａ）は、経路情報メモリ３５に元々記憶されている経路情報（ルーティングテーブル）をイメージ的に示したものである。テーブル中の○印は、経路が存在することを示している。通常は、ネットワーク２０上に接続されている各ノードに関する全ての経路が○印となっている。

【００６６】なお、第１の端末１から人事・給与サーバ１１に対する経路、第２の端末２から経理・財務サーバ１２に対する経路で“ＩＣ”と書かれているのは、ＩＣカード５，７を用いてユーザ認証を受けた場合にアクセスが許可される経路であることを示している。また、他のノードから人事・給与サーバ１１や経理・財務サーバ１２に対する経路も○印となっているが、これは単にそういう経路があるということを示しているだけで、アクセスを許可していることを意味するものではない。

【００６７】例えば、第１の端末１に関してユーザ認証が成立したとする。この場合は、第１の端末１が受信側となる部分の経路情報を図６（ｂ）のように置き換える。図６（ｂ）中の×印は、そのような経路が存在しないことを意味するものである。この置き換えは、他のノードから第１の端末１に至る経路情報を全て破棄することに相当する。この置き換えをするとき、元の経路情報を後から復元できるようにするために、置き換える前の経路情報を退避メモリ３６に退避させる。

【００６８】その後、第１の端末１においてＩＣカード５を抜くなどしてユーザ認証が解除されると、退避メモリ３６に退避しておいた元の経路情報を経路情報メモリ３５に戻すことにより、図６（ａ）の状態を復元する。なお、ユーザ認証の成立時に退避メモリ３６に退避させる経路情報は、図６（ａ）に示す経路情報全てであっても良いし、置き換える部分のみであっても良い。

【００６９】このように、第１の端末１に関してユーザ認証が成立している間は、他のノードから第１の端末１に至る経路の経路情報にマスクをかけることにより、アクセス要求元に対して、第１の端末１はあたかもネットワーク２０上に存在していないように見せることが可能となる。第１の端末１にアクセスする際には必ずルータ８を経由するが、ユーザ認証成立時にはそのルータ８内の経路情報を置き換えているので、外部から第１の端末１の存在を知ることはできず、第１の端末１にアクセスすることは一切できなくなる。

【００７０】したがって、例えば第３の端末３からユーザ認証が成立した第１の端末１をハッキングすることは全くできなくなり、第１の端末１を踏み台にして他人が第１の端末１のユーザになりすますことによる人事・給与サーバ１１への不正アクセスを有効に防止することができる。同様に、ユーザ認証が成立した第２の端末２をハッキングすることもできなくなり、第２の端末２を踏み台にした経理・財務サーバ１２への不正アクセスも有効に防止することができる。

【００７１】なお、第２の実施形態においても、例えば第１の端末１に関してユーザ認証が成立している間でも、ユーザ認証によりアクセスが許可された人事・給与サーバ１１からのアクセスだけは許可する（人事・給与

サーバ１１から第１の端末１に至る経路の経路情報はマスクしない）ようにすることも可能である。すなわち、図６（ｂ）の例で、下から２番目の部分は○印とする。

【００７２】図７は、第２の実施形態による不正アクセス防止装置３４の動作を示すフローチャートである。図７において、ルータ８内の制御部３３は、判断部３２を用いて、第１の端末１および第２の端末２に関してユーザ認証の成否（ユーザ認証の成立および解除）を監視している（ステップＳ１１）。

【００７３】第１の端末１および第２の端末２の双方ともユーザ認証が成立していない場合は、たとえこれらの端末１，２がハッキングされても、当該端末１，２を踏み台にして人事・給与サーバ１１や経理・財務サーバ１２にアクセスすることは不可能であるから、通常の経路情報を経路情報メモリ３５にそのまま保持し、ユーザ認証の成否を監視し続ける。これにより、第１の端末１および第２の端末２に対して外部から自由にアクセスすることが可能である。

【００７４】第１の端末１または第２の端末２に関してユーザ認証の成否に変化があったときは、それがユーザ認証の成立かどうかを判定する（ステップＳ１２）。第１の端末１または第２の端末２にユーザ認証が成立した場合には、そのユーザ認証が成立した端末に関する経路情報を経路情報メモリ３５から退避メモリ３６に退避し、当該端末に至る経路をマスクした第２の経路情報を経路情報メモリ３５に置き換える（ステップＳ１３）。

【００７５】一方、第１の端末１または第２の端末２に関してユーザ認証が解除された場合には、そのユーザ認証が解除された端末に関する経路情報を退避メモリ３６から経路情報メモリ３５に復元する（ステップＳ１４）。上記ステップＳ１３あるいはステップＳ１４の処理の後は、ステップＳ１１に戻ってユーザ認証成否の監視を継続する。

【００７６】以上詳しく説明したように、第２の実施形態においても、第１および第２の端末１，２に関してユーザ認証が成立している間は、これらの端末１，２に対する外部からのアクセスを遮断するように制御しているので、第１および第２の端末１，２をハッキングすることができないようにすることができる。これにより、第１および第２の端末１，２を踏み台にして他人が個人認証装置１３を通過し、人事・給与サーバ１１や経理・財務サーバ１２などに不正にアクセスすることを有効に防止することができる。

【００７７】なお、以上に説明した各実施形態は、何れも本発明を実施するにあたっての具体化の一例を示したものに過ぎず、これらによって本発明の技術的範囲が限定的に解釈されてはならないものである。すなわち、本発明はその精神、またはその主要な特徴から逸脱することなく、様々な形で実施することができる。例えば、第１の実施形態と第２の実施形態とを組み合わせて適用しても良い。

【００７８】

【発明の効果】本発明は上述したように、ネットワーク上に接続された端末に関してユーザ認証が成立している間は、そのユーザ認証が成立した端末に対する外部からのアクセスを遮断するように制御しているので、ユーザ認証が成立した端末をハッキングすることができないようにすることができる。これにより、ユーザ認証が成立した端末を踏み台に他人が正規利用者になりすまして目的のネットワークやシステムに不正にアクセスすることを有効に防止することができる。

【図面の簡単な説明】

【図１】第１および第２の実施形態による不正アクセス防止装置を適用したネットワークシステム全体の構成を示す図である。

【図２】第１の実施形態による第１の端末の機能構成例を示すブロック図である。

【図３】一般的な通信プロトコルを示す図である。

【図４】第１の実施形態による第１の端末に備えられる不正アクセス防止装置の動作を示すフローチャートである。

【図５】第２の実施形態によるルータの機能構成例を示すブロック図である。

【図６】経路情報の置き換え例を示す図である。

【図７】第２の実施形態によるルータに備えられる不正アクセス防止装置の動作を示すフローチャートである。

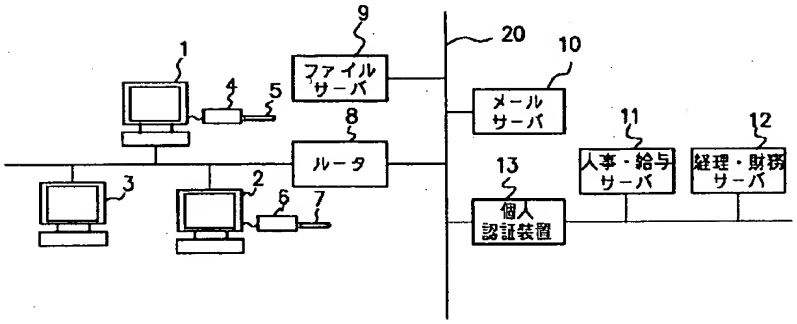
【図８】従来のネットワークシステム全体の構成を示す図である。

【符号の説明】

１，２，３　端末（パーソナルコンピュータ）
４，６　専用リーダ
５，７　ＩＣカード
８　ルータ
９　ファイルサーバ
１０　メールサーバ
１１　人事・給与サーバ
１２　経理・財務サーバ
１３　個人認証装置
２１　通信部
２２　認証処理部
２３　判断部
２４　制御部
２５　不正アクセス防止装置
３１　通信部
３２　判断部
３３　制御部
３４　不正アクセス防止装置
３５　経路情報メモリ
３６　退避メモリ

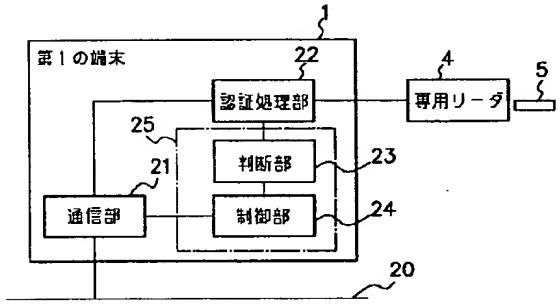
【図１】

ネットワークシステムの構成例



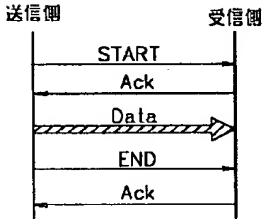
【図２】

第１の端末の機能構成例



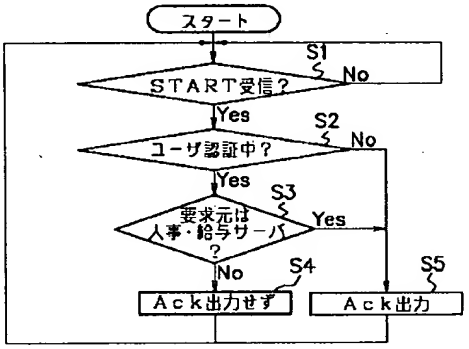
【図３】

通信のプロトコル



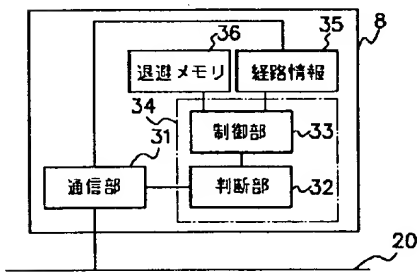
【図４】

第１の実施形態による動作フロー



【図５】

ルータの機能構成例



【図６】

経路情報の置換例

受信／発信	端末1	端末2	端末3	ファイル	メール	人・給	経・財
端末1		○	○	○	○	◎	○
端末2	○		○	○	○	○	◎
端末3	○	○		○	○	○	○
ファイル	○	○	○		○	○	○
メール	○	○	○	○		○	○
人・給	○	○	○	○	○		○
経・財	○	○	○	○	○	○	

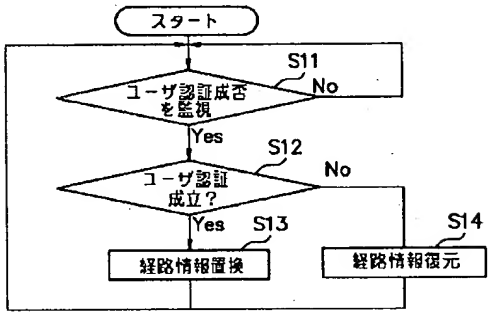
(a)

端末1
×
×
×
×
×
×

(b)

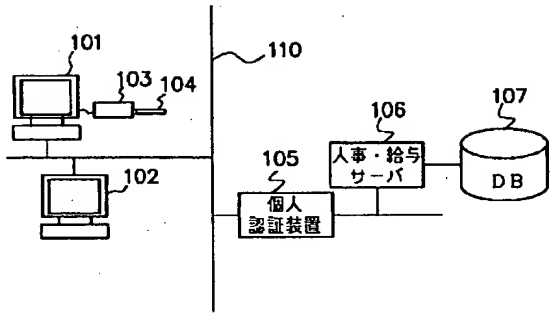
【図７】

第２の実施形態による動作フロー



【図８】

従来のネットワークシステム



フロントページの続き

Ｆターム(参考)　5B085 AE23 BG06
5J104 AA26 PA07
5K030 GA15 HA08 HC01 HC13 JT03
KA06 KA07 KA08 LA02 LC13

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-312316

(43)Date of publication of application : 25.10.2002

---

(51)Int.Cl. G06F 15/00

G06F 13/00

G09C 1/00

H04L 9/32

H04L 12/22

---

(21)Application number : 2001-114891 (71)Applicant : SUMISHO COMPUTER SYSTEMS CORP

(22)Date of filing : 13.04.2001 (72)Inventor : KATO MICHIAKI

---

(54) UNLAWFUL COMPUTER ACCESS PREVENTION DEVICE AND METHOD, UNLAWFUL COMPUTER ACCESS PREVENTION PROGRAM AND RECORDING MEDIUM

(57)Abstract:

PROBLEM TO BE SOLVED: To effectively prevent an unlawful computer access carried out by another person who successfully impersonates a correct user using a terminal in which a user certification is effected as a step.

SOLUTION: A judgment part 23 for judging whether or not the user certification is effected regarding a first terminal 1 connected onto a network 20 and a control part 24 for controlling it so as to disconnect an access from the outside to the first terminal 1 for the time when the user certification is effected (for example, a response is not returned even if an access requirement is sent to the first terminal 1 from the outside) are provided. The first terminal 1 cannot be hacked by disappearing the first terminal 1 in which the user certification is effected from

the outside. Thereby, it is effectively prevented that another person successfully impersonates the correct user using the first terminal 1 in which the user certification is effected as a step and unlawful computer accesses to the desired system.

LEGAL STATUS [Date of request for examination] 13.02.2003

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

CLAIMS

[Claim(s)]

[Claim 1] The unlawful access arrester characterized by to have the control means controlled to intercept access from the outside to the above-mentioned terminal when it is judged that the above-mentioned user authentication has been materialized with a decision means judge whether user authentication required to access the system on the above-mentioned network or the above-mentioned network has been materialized about the terminal connected on the network, and the above-mentioned decision means.

[Claim 2] It is the unlawful access arrester applied to the terminal equipped with the function to receive user authentication required to access the system on a network or the above-mentioned network. When the access request has been sent to the above-mentioned terminal from the exterior through the

above-mentioned network A decision means to judge whether the above-mentioned user authentication is materialized about the above-mentioned terminal, The unlawful access arrester characterized by having the control means controlled not to output the response to the above-mentioned access request when it is judged that the above-mentioned user authentication is materialized with the above-mentioned decision means.

[Claim 3] The above-mentioned control means is an unlawful access arrester according to claim 2 characterized by controlling not to output the response to the above-mentioned access request when the access request has been sent to the above-mentioned terminal through the above-mentioned network from the exteriors other than the system by which access was permitted by the above-mentioned user authentication while the above-mentioned user authentication is materialized about the above-mentioned terminal.

[Claim 4] It is the unlawful access arrester applied to the junction device on the network equipped with the function which judges and carries out data transfer of the following node transmitted with reference to path information based on a destination address. It is related with the terminal equipped with the function to receive user authentication required to access the system on the above-mentioned network or the above-mentioned network. When it is judged that the above-mentioned user authentication was materialized with a decision

means to judge whether the above-mentioned user authentication was materialized, and the above-mentioned decision means While transposing to the 2nd path information which intercepted the path which makes the destination the terminal with which the above-mentioned path information was evacuated and the above-mentioned user authentication was materialized The unlawful access arrester characterized by having the control means controlled to return the path information on the above 2nd to the path information on the origin which carried out [above-mentioned] evacuation when it is judged that the above-mentioned user authentication was canceled by the above-mentioned decision means.

[Claim 5] The path information on the above 2nd is an unlawful access arrester according to claim 4 characterized by being the path information for intercepting the path which made the above-mentioned terminal the destination from the exteriors other than the system by which access was permitted by the above-mentioned user authentication.

[Claim 6] When the access request has been sent to the terminal equipped with the function to receive user authentication required to access the system on a network or the above-mentioned network, through the above-mentioned network from the exterior The 1st step which judges whether the above-mentioned user authentication is materialized about the above-mentioned terminal, The unlawful access prevention approach characterized by having the 2nd step controlled not

to output the response to the above-mentioned access request when it is judged that the above-mentioned user authentication is materialized about the above-mentioned terminal.

[Claim 7] The unlawful access prevention approach according to claim 6 characterized by controlling by the 2nd step of the above not to output the response to the above-mentioned access request when the access request has been sent to the above-mentioned terminal through the above-mentioned network from the exteriors other than the system by which access was permitted by the above-mentioned user authentication while the above-mentioned user authentication is materialized about the above-mentioned terminal.

[Claim 8] It is related with the terminal equipped with the function to receive user authentication required to access the system on a network or the above-mentioned network. The 1st step which judges the success or failure of the above-mentioned user authentication, and when the above-mentioned user authentication is materialized about the above-mentioned terminal The 2nd step replaced with the 2nd path information which intercepted the path which makes the destination the terminal with which the above-mentioned path information of the data transfer junction [/ path information] device to the following node based on a destination address was evacuated, and the above-mentioned user authentication was materialized, The unlawful access prevention approach

characterized by having the 3rd step which returns the path information on the above 2nd to the path information on the origin which carried out [above-mentioned] evacuation when the above-mentioned user authentication is canceled about the above-mentioned terminal.

[Claim 9] The path information on the above 2nd is the unlawful access prevention approach according to claim 8 characterized by being the path information for intercepting the path which made the above-mentioned terminal the destination from the exteriors other than the system by which access was permitted by the above-mentioned user authentication.

[Claim 10] The unlawful access prevention program for operating a computer as a control means which controls to intercept access from the outside to the above-mentioned terminal, when it is judged that the above-mentioned user authentication has been materialized with a decision means judge whether user authentication required to access the system on the above-mentioned network or the above-mentioned network has been materialized about the terminal connected on the network, and the above-mentioned decision means.

[Claim 11] When the access request has been sent to the terminal equipped with the function to receive user authentication required to access the system on a network or the above-mentioned network, through the above-mentioned network from the exterior A decision means to judge whether the above-mentioned user

authentication is materialized about the above-mentioned terminal, And the unlawful access prevention program for operating a computer as a control means controlled not to output the response to the above-mentioned access request, when it is judged that the above-mentioned user authentication is materialized with the above-mentioned decision means.

[Claim 12] It is related with the terminal equipped with the function to receive user authentication required to access the system on a network or the above-mentioned network. When it is judged that the above-mentioned user authentication was materialized with the decision means and the above-mentioned decision means of judging whether the above-mentioned user authentication having been materialized The above-mentioned path information of the data transfer junction [/ path information] device to the following node based on a destination address is evacuated. When it is judged that the above-mentioned user authentication was canceled by the means replaced with the 2nd path information which intercepted the path which makes the destination the terminal with which the above-mentioned user authentication was materialized, and the above-mentioned decision means The unlawful access prevention program for operating a computer as a means to return the path information on the above 2nd to the path information on the origin which carried out [above-mentioned] evacuation.

[Claim 13] The record medium which is characterized by recording the program for operating a computer as each means of a publication on any 1 term of claims 10-12 and in which computer reading is possible.

DETAILED DESCRIPTION

[Detailed Description of the Invention]

[0001]

[Field of the Invention] This invention is applied to the junction device on the terminal equipped with the function to receive user authentication required to access the system on a network or the network concerned, and the network equipped with the function which judges and carries out data transfer of the following node transmitted with reference to path information based on a destination address, concerning an unlawful access arrester and an approach, the program for unlawful access prevention, and a record medium, and is suitable.

[0002]

[Description of the Prior Art] In recent years, the information system using networks, such as the Internet and intranet, is used widely. In this information

system, it has been an important technical problem how the unauthorized entry by others, an information leak, an alteration, operation active jamming of the information system itself, etc. are prevented. Although some techniques exist as a security system for keeping the insurance of an information system, a user authentication technique is in one of them.

[0003] The typical thing of a user authentication technique is a password. That is, each user enters from a keyboard etc. the password of a proper assigned to itself, and if the password is collated by the personal authentication system and the right thing is confirmed, it comes to be able to perform access to the system on a network or the system concerned.

[0004] However, a hacking technique improves in recent years and it is becoming easy to steal a password. Therefore, in user authentication with a password, it was impossible to have prevented unlawful access by others completely as a matter of fact. So, recently, the user authentication technique with which decode used the difficult IC card is also used increasingly. However, even if it used this IC card, after that IC card itself was stolen, there was a possibility of others having become a normal user, having cleared up and accessing unjustly.

[0005] From such the actual condition, recently, the so-called biometric-person-authentication technique of identifying an individual, especially

using a fingerprint, voice, a face, etc. attracts attention, and is developed. Moreover, the technique which combined this and an IC card is also developed. for example, a user's fingerprint data -- an IC card -- storing -- network utilization time -- the IC card -- a terminal -- inserting -- a user -- his fingerprint data are collated, and if right, access to a network etc. will be permitted.

[0006]

[Problem(s) to be Solved by the Invention] According to an above-mentioned biometric-person-authentication technique, the user authentication technique which combined this and an IC card, compared with the case where a conventional password and a conventional IC card are used alone, it is possible to raise the safety of an information system. However, however it might make full use of a user authentication technique, when the terminal with which user authentication was materialized was hacked, the terminal was made a steppingstone and there was a problem that unjust access by others will be performed.

[0007] This is explained in detail using drawing 8 . In the system shown in drawing 8 , the 1st and 2nd terminal 101,102, and personnel affairs and a salary server 106 are connected through the network 110. The database 107 is connected to personnel affairs and the salary server 106, and the various data about personnel affairs and a salary are stored. In these various data, the

individual humanity news about individual school education, punishment, clinical recording, health condition, salary, etc. is also contained.

[0008] Personal authentication equipment 105 is installed between the 1st and 2nd terminal 101,102, and personnel affairs and a salary server 106. That it should avoid un-arranging [that the data on a database 107 are altered or individual humanity news is stolen], personal authentication equipment 105 performs processing about user authentication, in order to permit access to personnel affairs and the salary server 106 only to a specific user.

[0009] The exclusive reader 103 of IC card 104 is connected to the 1st terminal 101. The authentication information (biotechnology information, such as a user's status information or a fingerprint etc.) about the user who has an access privilege to personnel affairs and the salary server 106 is stored in IC card 104.

[0010] When the user of the 1st terminal 101 accesses personnel affairs and the salary server 106 through a network 110, IC card 104 is inserted in the exclusive reader 103, and the 1st terminal 101 is made to read one's authentication information first. The 1st terminal 101 sends the read authentication information to personal authentication equipment 105. Personal authentication equipment 105 checks the authentication information sent from the 1st terminal 101, and if right, it will permit access to personnel affairs and the salary server 106.

[0011] Thus, if user authentication is materialized to the 1st terminal 101, the

pass from the 1st terminal 101 concerned to personnel affairs and the salary server 106 through personal authentication equipment 105 will be formed. In this condition, if the 1st terminal 101 is hacked from the 2nd terminal 102, the 1st terminal 101 will be made a steppingstone and the user of the 2nd terminal 102 will be possible [accessing unjustly at spoofing and personnel affairs and a salary server 106 at the user of the 1st terminal 1].

[0012] Thus, it is becoming difficult conventionally for amelioration to be added and, as for the user authentication technique itself, for others other than a normal user to receive user authentication. However, by hacking the terminal to which user authentication was materialized by the normal user, the terminal concerned will be made a steppingstone and it will enable them for others to become a normal user and to clear up. Therefore, unlawful access by others to the system on a network or the network concerned was not able to be prevented completely.

[0013] This invention is accomplished in order to solve such a problem, makes a steppingstone the terminal with which user authentication was materialized, and aims at enabling it to prevent effectively unlawful access that others become a normal user and clear up.

[0014]

[Means for Solving the Problem] The unlawful access arrester of this invention is

characterized by to have the control means controlled to intercept access from the outside to the above-mentioned terminal, when it is judged that the above-mentioned user authentication has been materialized with a decision means judge whether user authentication required to access the system on the above-mentioned network or the above-mentioned network has been materialized about the terminal connected on the network, and the above-mentioned decision means.

[0015] It is the unlawful access arrester applied to the terminal equipped with the function to receive user authentication required in other modes of this invention to access the system on a network or the above-mentioned network. When the access request has been sent to the above-mentioned terminal from the exterior through the above-mentioned network It is characterized by having a decision means to judge whether the above-mentioned user authentication is materialized about the above-mentioned terminal, and the control means controlled not to output the response to the above-mentioned access request when it is judged that the above-mentioned user authentication is materialized with the above-mentioned decision means.

[0016] In the mode of others of this invention, the above-mentioned control means is characterized by controlling not to output the response to the above-mentioned access request, when the access request has been sent to the

above-mentioned terminal through the above-mentioned network from the exteriors other than the system by which access was permitted by the above-mentioned user authentication while the above-mentioned user authentication is materialized about the above-mentioned terminal.

[0017] In the mode of others of this invention, path information is referred to based on a destination address. It is the unlawful access arrester applied to the junction device on the network equipped with the function which judges and carries out data transfer of the following node to transmit. It is related with the terminal equipped with the function to receive user authentication required to access the system on the above-mentioned network or the above-mentioned network. When it is judged that the above-mentioned user authentication was materialized with a decision means to judge whether the above-mentioned user authentication was materialized, and the above-mentioned decision means While transposing to the 2nd path information which intercepted the path which makes the destination the terminal with which the above-mentioned path information was evacuated and the above-mentioned user authentication was materialized When it is judged that the above-mentioned user authentication was canceled by the above-mentioned decision means, it is characterized by having the control means controlled to return the path information on the above 2nd to the path information on the origin which carried out [above-mentioned]

evacuation.

[0018] In the mode of others of this invention, path information on the above 2nd is characterized by being the path information for intercepting the path which made the above-mentioned terminal the destination from the exteriors other than the system by which access was permitted by the above-mentioned user authentication.

[0019] Moreover, when the access request has been sent to the terminal equipped with the function to receive user authentication required to access the system on a network or the above-mentioned network, through the above-mentioned network from the exterior, the unlawful access prevention approach of this invention It is characterized by having the 1st step which judges whether the above-mentioned user authentication is materialized about the above-mentioned terminal, and the 2nd step controlled not to output the response to the above-mentioned access request when it is judged that the above-mentioned user authentication is materialized about the above-mentioned terminal.

[0020] In other modes of this invention, at the 2nd step of the above, when the access request has been sent to the above-mentioned terminal through the above-mentioned network from the exteriors other than the system by which access was permitted by the above-mentioned user authentication while the

above-mentioned user authentication is materialized about the above-mentioned terminal, it is characterized by controlling not to output the response to the above-mentioned access request.

[0021] It is related with the terminal equipped with the function to receive user authentication required in the mode of others of this invention to access the system on a network or the above-mentioned network. The 1st step which judges the success or failure of the above-mentioned user authentication, and when the above-mentioned user authentication is materialized about the above-mentioned terminal The 2nd step replaced with the 2nd path information which intercepted the path which makes the destination the terminal with which the above-mentioned path information of the data transfer junction [/ path information] device to the following node based on a destination address was evacuated, and the above-mentioned user authentication was materialized, When the above-mentioned user authentication is canceled about the above-mentioned terminal, it is characterized by having the 3rd step which returns the path information on the above 2nd to the path information on the origin which carried out [above-mentioned] evacuation.

[0022] In the mode of others of this invention, path information on the above 2nd is characterized by being the path information for intercepting the path which made the above-mentioned terminal the destination from the exteriors other than

the system by which access was permitted by the above-mentioned user authentication.

[0023] Moreover, the unlawful access prevention program of this invention is for operating a computer as a control means which controls to intercept access from the outside to the above-mentioned terminal, when it is judged that the above-mentioned user authentication has been materialized with a decision means judge whether user authentication required to access the system on the above-mentioned network or the above-mentioned network has been materialized about the terminal connected on the network, and the above-mentioned decision means.

[0024] When the access request has been sent to the terminal equipped with the function to receive user authentication required in other modes of this invention to access the system on a network or the above-mentioned network, through the above-mentioned network from the exterior A decision means to judge whether the above-mentioned user authentication is materialized about the above-mentioned terminal, And when it is judged that the above-mentioned user authentication is materialized with the above-mentioned decision means, it is characterized by operating a computer as a control means controlled not to output the response to the above-mentioned access request.

[0025] It is related with the terminal equipped with the function to receive user

authentication required in the mode of others of this invention to access the system on a network or the above-mentioned network. When it is judged that the above-mentioned user authentication was materialized with the decision means and the above-mentioned decision means of judging whether the above-mentioned user authentication having been materialized The above-mentioned path information of the data transfer junction [/ path information] device to the following node based on a destination address is evacuated. When it is judged that the above-mentioned user authentication was canceled by the means replaced with the 2nd path information which intercepted the path which makes the destination the terminal with which the above-mentioned user authentication was materialized, and the above-mentioned decision means It is characterized by operating a computer as a means to return the path information on the above 2nd to the path information on the origin which carried out [above-mentioned] evacuation.

[0026] Moreover, the record medium which can computer read this invention is characterized by recording the program for operating a computer as each means of a publication on any 1 term of claims 10-12.

[0027]

[Embodiment of the Invention] (1st operation gestalt) The 1st operation gestalt of this invention is hereafter explained based on a drawing. Drawing 1 is drawing

showing the configuration of the whole network system which applied the unlawful access arrester by this operation gestalt.

[0028] In drawing 1 , personnel affairs and a salary server, and 12 are connected so that a file server and 10 may be accounting and a financial server a mail server and 11 and, as for the terminal with which 1, 2, and 3 consist of a personal computer etc., and 9, these can communicate mutually through a network 20.

[0029] A file server 9 processes transfer of a file, deletion, directory actuation, etc. A mail server 10 performs processing handed over when the electronic mail was transmitted, or the delivered electronic mail is kept and there is enquiry from terminals 1, 2, and 3 based on the demand from terminals 1, 2, and 3. Personnel affairs and the salary server 11 perform various processings about the personnel affairs and the salary in a company. Accounting and the financial server 12 perform various processings about the accounting and financial affairs in a company. In addition, since these various servers 9-12 can use a well-known thing, detailed explanation of the contents of processing is omitted here.

[0030] 8 is a router and is installed in the suitable location on a network 20. The data transmitted on the network 20 from a certain computer are surely sent to the target computer via a router 8. This router 8 judges the following node to transmit based on the destination IP address in IP header with reference to the

path information (routing table) which router 8 self has, and transmits data.

[0031] 13 is personal authentication equipment and is installed between the 1st - the 3rd terminal 1-3, and personnel affairs, the salary server 11 and accounting and a financial server 12. Personal authentication equipment 13 performs processing about user authentication based on the authentication information sent from the 1st and 2nd terminals 1 and 2, in order to permit access to personnel affairs and the salary server 11, and accounting and a financial server 12 only to a specific user.

[0032] The exclusive reader 4 of IC card 5 is connected to the 1st terminal 1. The authentication information (biotechnology information, such as a user's status information or a fingerprint etc.) about the user who has an access privilege to personnel affairs and the salary server 11 is stored in IC card 5. The user of the 1st terminal 1 can also access personnel affairs and the salary server 11 by receiving user authentication using IC card 5 while being able to access a file server 9 and a mail server 10 freely.

[0033] When the user of the 1st terminal 1 accesses personnel affairs and the salary server 11, IC card 5 is inserted in the exclusive reader 4, and the 1st terminal 1 is made to read one's authentication information first. The 1st terminal 1 sends the read authentication information to personal authentication equipment 13 through a router 8. Personal authentication equipment 13 checks

the authentication information sent from the 1st terminal 1, and if right, it will permit access to personnel affairs and the salary server 11.

[0034] Moreover, the exclusive reader 6 of IC card 7 is connected to the 2nd terminal 2. The authentication information (biotechnology information, such as a user's status information or a fingerprint etc.) about the user who has an access privilege to accounting and the financial server 12 is stored in IC card 7. The user of the 2nd terminal 2 can also access accounting and the financial server 12 by receiving user authentication using IC card 7 while being able to access a file server 9 and a mail server 10 freely.

[0035] When the user of the 2nd terminal 2 accesses accounting and the financial server 12, IC card 7 is inserted in the exclusive reader 6, and the 2nd terminal 2 is made to read one's authentication information first. The 2nd terminal 2 sends the read authentication information to personal authentication equipment 13 through a router 8. Personal authentication equipment 13 checks the authentication information sent from the 2nd terminal 2, and if right, it will permit access to accounting and the financial server 12.

[0036] The 3rd terminal 3 is not equipped with the function for receiving user authentication. That is, it does not have an access privilege to personnel affairs, the salary server 11, and accounting and a financial server 12, but the user of the 3rd terminal 3 can be accessed only to a file server 9 and a mail server 10.

[0037] In addition, although considered as the configuration which forms the exclusive readers 4 and 6 of IC cards 5 and 7 by external [of the 1st and 2nd terminals 1 and 2] here, the 1st and 2nd terminals 1 and 2 the very thing may be equipped with the reading function of IC cards 5 and 7. Moreover, although IC cards 5 and 7 are used in order to receive user authentication here, this invention does not limit especially the approach of user authentication. For example, other user authentication techniques, such as a password, may be used.

[0038] Moreover, although what needs user authentication for accessing was made into personnel affairs, the salary server 11, and accounting and a financial server 12, it is not limited to these servers here. For example, it may be made to consider as the prerequisite of access to the user authentication by personal authentication equipment 13 also with other servers or file servers 9 which are not illustrated, a mail server 10, or the host computer which is not illustrated.

[0039] Drawing 2 is the block diagram showing the example of a functional configuration of the 1st terminal 1. In addition, since it is constituted like [the 2nd terminal 2] the 1st terminal 1, illustration is omitted here. In drawing 2 , 21 is the communications department and performs processing about transmission and reception of data through a network 20. 22 is the authentication processing section, moves together with personal authentication equipment 13, and

performs processing about user authentication.

[0040] The above-mentioned authentication processing section 22 incorporates the authentication information in IC card 5 read by the exclusive reader 4, and has the function transmitted to personal authentication equipment 13 through the communications department 21. Moreover, the authentication authorization information sent through the communications department 21 from personal authentication equipment 13 is incorporated, and it also has the function to hold. Only while the authentication processing section 22 holds authentication authorization information, it is possible to access personnel affairs and the salary server 11.

[0041] 23 is the decision section, and when the access request has been sent to the communications department 21 through a network 20 from the exterior, it judges whether user authentication is materialized about the 1st terminal 1 by seeing authentication authorization information whether held by the authentication processing section 22.

[0042] In addition, although authentication authorization information is made to hold in the authentication processing section 22 here and the success or failure of user authentication are judged by the existence of the information concerned, this invention is not limited to this example. For example, when the access request has been sent from the exterior, you may make it ask personal

authentication equipment 13 the success or failure of user authentication through the communications department 21. In this case, personal authentication equipment 13 will hold authentication authorization information.

[0043] 24 is a control section, and when the access request has been sent to the 1st terminal 1 through a network 20 from the exterior while user authentication is materialized about the 1st terminal 1, it is controlled not to output the response to the access request from the communications department 21. On the other hand, when user authentication is not materialized about the 1st terminal 1, it usually passes and controls to output a response to the access request from the outside.

[0044] The unlawful access arrester 25 of this operation gestalt is constituted by the above-mentioned decision section 23 and the control section 24. This unlawful access arrester 25 consists of a CPU of the 1st terminal 1, MPU, RAM, ROM, etc. in fact, and the functional configuration of the decision section 23 and the control section 24 which were mentioned above when the program memorized by RAM and ROM operated is realized.

[0045] Therefore, the program operated so that the 1st terminal 1 may achieve the function of the above-mentioned decision section 23 and a control section 24 is recorded on a record medium like CD-ROM, and it can realize by making it read into a computer. As a record medium which records the above-mentioned program, a floppy (trademark) disk, a hard disk, a magnetic tape, an optical disk,

a magneto-optic disk, DVD, a non-volatile memory card, etc. can be used in addition to CD-ROM. Moreover, you may make it download the above-mentioned program from other computers through a network 20.

[0046] moreover, the function of the decision section 23 and a control section 24 is not only realized by performing the program to which the 1st terminal 1 was supplied, but The case where an above-mentioned function is realized in collaboration with OS (operating system) or other application software etc. with which the program is working in the 1st terminal 1, Also when all or a part of supplied processing of a program is performed by the 1st functional add-in board and functional expansion unit of a terminal 1 and an above-mentioned function is realized, this program is included in the operation gestalt of this invention.

[0047] Drawing 3 is drawing showing a general communications protocol. When transmitting data to a receiving side from a transmitting side, the signal START which tells starting data transmission is first sent to a receiving side from a transmitting side. If a reply signal Ack is returned to a transmitting side from a receiving side corresponding to this, Data Data will be sent to a receiving side from a transmitting side. Termination of data transmission sends the signal END which tells that data transmission was completed to a receiving side from a transmitting side. A series of data communication is completed by returning a reply signal Ack to a transmitting side from a receiving side corresponding to this.

[0048] In such a communications protocol, a control section 24 is controlled not to return the reply signal Ack over it, when the data transmitting start signal START which is an access request has been sent from the outside while user authentication is materialized about the 1st terminal 1. By doing in this way, the 1st terminal 1 becomes possible [showing as it does not exist on a network 20] to access request origin.

[0049] Usually, hacking to the 1st terminal 1 with which user authentication is materialized sends temporary data to the 1st terminal 1 from the exterior, and is performed by checking the existence location on the network 20 of the 1st terminal 1. However, since a response is not returned to the access request from the outside while user authentication is materialized, the 1st terminal 1 existence of the 1st terminal 1, and it becomes impossible [the terminal] according to this operation gestalt entirely to access the 1st terminal 1. [exterior]

[0050] It completely becomes impossible to hack the 1st terminal 1 with which it followed, for example, user authentication was materialized from the 3rd terminal 3, it can make the 1st terminal 1 a steppingstone, and can prevent effectively unlawful access to the personnel affairs and the salary server 11 by others becoming the user of the 1st terminal 1 and clearing up. Unlawful access to the accounting and the financial server 12 which it also becomes impossible similarly to have hacked the 2nd terminal 2 with which user authentication was

materialized, and made the 2nd terminal 2 a steppingstone can also be prevented effectively.

[0051] Although it is possible to access personnel affairs and the salary server 11 from the 1st terminal 1 while user authentication is materialized, for example about the 1st terminal 1, it becomes impossible to access the 1st terminal 1 from personnel affairs and the salary server 11 conversely in the above example. However, a timer is set to Nighttime, for example and demand of printing by starting from personnel affairs and the salary server 11, and sending desired data to the 1st terminal 1 also exists.

[0052] Since it corresponds to such a demand, also while user authentication is materialized about the 1st terminal 1, the thing to which a permission is granted and which is made like (a reply signal Ack is returned) is also possible only for access from the personnel affairs and the salary server 11 to which access was permitted by user authentication. That is, the control section 24 in this case is controlled not to output the response to that access request, when the access request has been sent to the 1st terminal 1 through a network 20 from computers personnel affairs and other than salary server 11.

[0053] Drawing 4 is a flow chart which shows actuation of the unlawful access arrester 25 with which the 1st terminal 1 in this case is equipped. In drawing 4 , a control section 24 judges whether user authentication is materialized about the

1st terminal 1 of the present using the decision section 23, when the communications department 21 supervises whether the data transmitting start signal START was received from the exterior (step S1) and receives this (step S2).

[0054] When current user authentication is not materialized, even if the 1st terminal 1 is hacked, since it is impossible, making the 1st terminal 1 concerned a steppingstone and accessing personnel affairs and the salary server 11 will control the communications department 21 to usually pass and to return a reply signal Ack (step S5). This becomes possible to access freely from the outside to the 1st terminal 1.

[0055] On the other hand, when current user authentication is materialized, a control section 24 judges whether access request origin (data transmitting start signal START dispatch-origin) is personnel affairs and the salary server 11 (step S3). When performing user authentication using IC card 5 like this operation gestalt and setting authentication information as the IC card 5, the IP address of personnel affairs and the salary server 11 is also held. Therefore, it is possible to judge whether access request origin is personnel affairs and the salary server 11 by obtaining whether the IP address read in IC card 5 and the IP address sent with the data transmitting start signal START are in agreement.

[0056] When access request origin is not personnel affairs and the salary server

11, a control section 24 controls the communications department 21 not to return a reply signal Ack to the data transmitting start signal START (step S4). Thereby, it is made for the 1st terminal 1 not to appear from the outside, and unlawful access to the personnel affairs and the salary server 11 which made the 1st terminal 1 a steppingstone is prevented.

[0057] Moreover, when access request origin is personnel affairs and the salary server 11, a control section 24 controls the communications department 21 to return a reply signal Ack to the data transmitting start signal START (step S5). This becomes possible to access to personnel affairs and the salary server 11 freely to the 1st terminal 1.

[0058] Since it is controlling in the 1st operation gestalt to intercept access from the outside to these terminals 1 and 2 while user authentication is materialized about the 1st and 2nd terminals 1 and 2 as explained in detail above, it can avoid hacking the 1st and 2nd terminals 1 and 2. By this, the 1st and 2nd terminals 1 and 2 can be made a steppingstone, others can pass personal authentication equipment 13, and it can prevent effectively accessing unjustly personnel affairs and the salary server 11, accounting, a financial server 12, etc.

[0059] (2nd operation gestalt) Next, the 2nd operation gestalt of this invention is explained based on a drawing. The configuration of the whole network system which applied the unlawful access arrester by the 2nd operation gestalt is the

same as that of drawing 1 . However, the 1st and 2nd terminals 1 and 2 are not equipped with the functional configuration of the unlawful access arrester 25 shown in drawing 2 . In this operation gestalt, an unlawful access arrester is formed in a router 8.

[0060] Drawing 5 is the block diagram showing the example of a functional configuration of a router 8. In drawing 5 , 31 is the communications department and performs processing about data transfer through a network 20. That is, with reference to the path information (routing table) currently held at the path information memory 35, the following node to transmit is judged based on the destination IP address in IP header of the data sent through a network 20, and data are transmitted.

[0061] 32 is the decision section and judges the success or failure of the user authentication about the 1st terminal 1 and 2nd terminal 2. When the 1st and 2nd terminals 1 and 2 receive user authentication, data required for user authentication are exchanged via a router 8 among these terminals 1 and 2 and personal authentication equipment 13. Therefore, when the decision section 32 supervises the data which mind the communications department 31 of a router 8 in the case of activation of user authentication, and are carried out at it, it is possible to check that user authentication was materialized or that user authentication has been canceled after that.

[0062] In addition, the technique of judging the success or failure of the user authentication about the 1st and 2nd terminals 1 and 2 is not limited to this. For example, when user authentication is materialized or canceled by the 1st and 2nd terminals 1 and 2, you may make it tell that clearly to a router 8 from the 1st and 2nd terminals 1 and 2.

[0063] 33 is a control section, when it is judged that user authentication was materialized about the 1st terminal 1 or 2nd terminal 2 by the decision section 32, evacuates the path information in the path information memory 35 to the evacuation memory 36, and transposes the contents of the path information memory 35 to the 2nd path information which intercepted the path which makes the destination the terminal with which user authentication was materialized. Moreover, when it is judged that user authentication was canceled, it controls to return the path information on the origin which evacuated to the evacuation memory 36 to the path information memory 35.

[0064] The unlawful access arrester 34 of this operation gestalt is constituted by the above-mentioned decision section 32 and the control section 33. This unlawful access arrester 34 consists of a CPU of a router 8, MPU, RAM, ROM, etc. in fact, and the functional configuration of the decision section 32 and the control section 33 which were mentioned above when the program memorized by RAM and ROM operated is realized.

[0065] Drawing 6 is drawing showing the example of replacement of path information. Drawing 6 (a) shows in image the path information (routing table) memorized from the first by the path information memory 35. O mark in a table shows that a path exists. Usually, all the paths about each node connected on the network 20 serve as O mark.

[0066] In addition, from the 1st terminal 1, being written as "IC" in the path over accounting and the financial server 12 from the path and the 2nd terminal 2 over personnel affairs and the salary server 11 shows that it is the path to which access is permitted, when user authentication is received using IC cards 5 and 7. Moreover, although the path over personnel affairs and the salary server 11, or accounting and a financial server 12 also serves as O mark from other nodes, it does not mean that this only shows that there is only such a path, and has permitted access.

[0067] For example, suppose that user authentication was materialized about the 1st terminal 1. In this case, the path information on a part that the 1st terminal 1 serves as a receiving side is replaced like drawing 6 (b). x mark in drawing 6 (b) means that such a path does not exist. This replacement is equivalent to canceling all the path information from other nodes to the 1st terminal 1. When carrying out this replacement, in order to enable it to restore the path information on original later, the path information before replacing is

evacuated to the evacuation memory 36.

[0068] Then, if IC card 5 is extracted in the 1st terminal 1 and user authentication is canceled, the condition of drawing 6 (a) will be restored by returning the path information on the origin which evacuated to the evacuation memory 36 to the path information memory 35. In addition, the path information evacuated to the evacuation memory 36 at the time of formation of user authentication may be all path information shown in drawing 6 (a), and may be only parts to replace.

[0069] Thus, while user authentication is materialized about the 1st terminal 1, the 1st terminal 1 becomes possible [showing as it does not exist on a network 20] to access request origin by covering a mask over the path information on a path that it results [from other nodes] in the 1st terminal 1. Although it surely goes via a router 8 in case the 1st terminal 1 is accessed, since the path information in the router 8 is replaced at the time of user authentication formation, existence of the 1st terminal 1 cannot be known from the exterior, but it becomes impossible entirely to access the 1st terminal 1.

[0070] It completely becomes impossible to hack the 1st terminal 1 with which it followed, for example, user authentication was materialized from the 3rd terminal 3, it can make the 1st terminal 1 a steppingstone, and can prevent effectively unlawful access to the personnel affairs and the salary server 11 by others becoming the user of the 1st terminal 1 and clearing up. Unlawful access to the

accounting and the financial server 12 which it also becomes impossible similarly to have hacked the 2nd terminal 2 with which user authentication was materialized, and made the 2nd terminal 2 a steppingstone can also be prevented effectively.

[0071] In addition, also in the 2nd operation gestalt, also while user authentication is materialized, for example about the 1st terminal 1, the thing to which a permission is granted and which is made like (the mask of the path information on a path that it results [from personnel affairs and the salary server 11] in the 1st terminal 1 is not carried out) is also possible only for access from the personnel affairs and the salary server 11 to which access was permitted by user authentication. That is, the 2nd part is considered as O mark from the bottom in the example of drawing 6 (b).

[0072] Drawing 7 is a flow chart which shows actuation of the unlawful access arrester 34 by the 2nd operation gestalt. In drawing 7 , the control section 33 in a router 8 is supervising the success or failure (formation and discharge of user authentication) of user authentication about the 1st terminal 1 and 2nd terminal 2 using the decision section 32 (step S11).

[0073] When user authentication is not materialized by the both sides of the 1st terminal 1 and the 2nd terminal 2, even if these terminals 1 and 2 are hacked, since it is impossible, making the terminals 1 and 2 concerned a steppingstone

and accessing them at personnel affairs and the salary server 11, or accounting and a financial server 12 will hold the usual path information as it is in the path information memory 35, and it will continue supervising the success or failure of user authentication. It is possible for this to access freely from the outside to the 1st terminal 1 and 2nd terminal 2.

[0074] When the success or failure of user authentication have change about the 1st terminal 1 or 2nd terminal 2, it judges whether it is formation of user authentication (step S12). When user authentication is materialized to the 1st terminal 1 or 2nd terminal 2, the path information about the terminal with which the user authentication was materialized is evacuated from the path information memory 35 to the evacuation memory 36, and the 2nd path information which carried out the mask of the path which results in the terminal concerned is transposed to the path information memory 35 (step S13).

[0075] On the other hand, when user authentication is canceled about the 1st terminal 1 or 2nd terminal 2, the path information about the terminal of which the user authentication was canceled is restored to the path information memory 35 from the evacuation memory 36 (step S14). After processing of the above-mentioned step S13 or step S14 returns to step S11, and continues the monitor of user authentication success or failure.

[0076] Since it is controlling also in the 2nd operation gestalt to intercept access

from the outside to these terminals 1 and 2 while user authentication is materialized about the 1st and 2nd terminals 1 and 2 as explained in detail above, it can avoid hacking the 1st and 2nd terminals 1 and 2. By this, the 1st and 2nd terminals 1 and 2 can be made a steppingstone, others can pass personal authentication equipment 13, and it can prevent effectively accessing unjustly personnel affairs and the salary server 11, accounting, a financial server 12, etc.

[0077] In addition, it passes over no each operation gestalten explained above to what showed an example of the somatization which hits carrying out this invention, and the technical range of this invention must not be restrictively interpreted by these. That is, this invention can be carried out in various forms, without deviating from the pneuma or its main description. For example, you may apply combining the 1st operation gestalt and the 2nd operation gestalt.

[0078]

[Effect of the Invention] Since this invention is controlled to intercept access from the outside to the terminal with which the user authentication was materialized while user authentication is materialized about the terminal connected on the network, as mentioned above, it can avoid hacking the terminal with which user authentication was materialized. It can prevent effectively others becoming to a normal user at a step, clearing up the terminal with which user authentication

was materialized, and accessing unjustly by this, at a target network and a target system.

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]

[Drawing 1] It is drawing showing the configuration of the whole network system which applied the unlawful access arrester by the 1st and 2nd operation gestalten.

[Drawing 2] It is the block diagram showing the example of a functional configuration of the 1st terminal by the 1st operation gestalt.

[Drawing 3] It is drawing showing a general communications protocol.

[Drawing 4] It is the flow chart which shows actuation of the unlawful access arrester with which the 1st terminal by the 1st operation gestalt is equipped.

[Drawing 5] It is the block diagram showing the example of a functional configuration of the router by the 2nd operation gestalt.

[Drawing 6] It is drawing showing the example of replacement of path information.

[Drawing 7] It is the flow chart which shows actuation of the unlawful access

arrester with which the router by the 2nd operation gestalt is equipped.

[Drawing 8] It is drawing showing the configuration of the conventional whole network system.

[Description of Notations]

1, 2, 3 Terminal (personal computer)

4 Six Exclusive reader

5 Seven IC card

8 Router

9 File Server

10 Mail Server

11 Personnel Affairs and Salary Server

12 Accounting and Financial Server

13 Personal Authentication Equipment

21 Communications Department

22 Authentication Processing Section

23 Decision Section

24 Control Section

25 Unlawful Access Arrester

31 Communications Department

32 Decision Section

33 Control Section

34 Unlawful Access Arrester

35 Path Information Memory

36 Evacuation Memory